UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

| | |
|---|---|
| BERNADINE GRIFFITH et al.,<br><br>Plaintiffs,<br><br>v.<br><br>TIKTOK, INC. et al.,<br><br>Defendants. | **UNDER SEAL**[1]<br><br>Case No. 5:23-cv-00964-SB-E<br><br>ORDER DENYING MOTION FOR CLASS CERTIFICATION [DKT. NO. 177] |

In this putative class action, Plaintiffs challenge Defendants TikTok, Inc. and ByteDance, Inc.'s use of software to collect information about non-TikTok users' internet activity when they visit third-party websites that have installed Defendants' software. Following two rounds of pleading challenges, Plaintiffs move for certification of two alternative sets of classes and subclasses. Dkt. No. 177. The Court held a hearing on the motion on August 16, 2024.

As to the first set of classes proposed by Plaintiffs, which attempt to encompass visitors to the hundreds of thousands of websites that use Defendants' software, Plaintiffs have not shown that the named plaintiffs are typical of the class or that common issues will predominate. The parties devote scant attention to the

[1] Because some of the briefing and exhibits filed in connection with the motion for class certification are under seal, the Court has preliminarily sealed this order. The Court expects to unseal the order unless the parties show a compelling reason not to. Within four business days after entry of this order, the parties shall meet and confer and file a joint statement as to whether any part of this opinion should remain sealed. If the parties do not agree that the order should be unsealed in its entirety, they shall propose specific redactions and explain the need for each redaction sought.

second set of proposed classes, which focus on five specific websites visited by the named plaintiffs. While it may be possible for Plaintiffs to show that certification is appropriate as to those classes, they have not done so on this record. Accordingly, their motion is denied.

I.

The allegations in this case are addressed in depth in the Court's orders on Defendants' motions to dismiss the original complaint and the First Amended Complaint (FAC). Dkt. Nos. 59, 81. After those rulings, which dismissed Plaintiffs' claims for unjust enrichment and for violations of the federal Computer Fraud and Abuse Act and California's Unfair Competition Law, the parties stipulated to the filing of Plaintiffs' Second Amended Complaint (SAC), which substituted a named plaintiff but did not otherwise alter the nature of Plaintiffs' surviving claims. In the SAC, Plaintiffs Bernadette Griffith, Patricia Shih, Philip Cantore, and Jacob Watters allege claims for (1) violation of the California Invasion of Privacy Act (CIPA), (2) statutory larceny under §§ 484 and 496 of the California Penal Code, (3) conversion, (4) invasion of privacy under the California Constitution, (5) intrusion on seclusion, and (6) violation of the Electronic Communication Privacy Act (ECPA). Dkt. No. 137.[2]

As clarified in the class certification submissions, Plaintiffs' claims focus on two distinct types of software provided by Defendants for use by third parties on their websites: the Pixel, which is installed on hundreds of thousands of websites, and Events API, which is somewhat less widely used. The Pixel is embedded on the third-party website, while Events API sends information directly from the third party's server to Defendants' server without involving the browser in the communication. Both tools collect and send to Defendants[3] information about all website visitors, regardless of whether they are TikTok users, and Defendants then

[2] The SAC also realleged a claim for unjust enrichment, which the Court dismissed without opposition from Plaintiffs at the August 16 hearing, based on its earlier dismissal of that claim in the FAC. Dkt. No. 229 at 2.

[3] Defendants assert in a footnote to their opposition that TikTok, Inc. is the entity that offers the TikTok platform in the United States and that Plaintiffs have improperly conflated the two defendant entities. Because Plaintiffs do not distinguish between Defendants in their argument, the Court addresses them together without making any finding as to the propriety of Plaintiffs' approach.

attempt to match the data to their records of TikTok users. Defendants maintain that the information collected from non-TikTok users is valueless to them and ultimately deleted but that they are unable to exclude the nonusers' data in advance because of how the software works.

The SAC identifies seven organizations' websites that installed the TikTok Pixel and that the named plaintiffs visited during the class period: Rite Aid, Hulu, Etsy, Build-a-Bear, Upwork, The Vitamin Shoppe, and Feeding America. Plaintiffs now seek to certify classes with respect to four of these—Rite Aid, Hulu, Etsy, and Upwork—and a fifth website (Sweetwater) not mentioned in the SAC. Alternatively, Plaintiffs seek to certify a series of classes and subclasses involving all websites that use the TikTok Pixel.

II.

Before turning to the motion, the Court first addresses a significant factual dispute that arose at the class certification hearing. Plaintiffs' counsel contended that Defendants collect information that would allow them to identify every single non-TikTok user who visits a site with the TikTok Pixel installed. When pressed by the Court, counsel represented that the data would permit Defendants to identify the non-users by name:

> The Court: I'm asking whether or not from the record before me TikTok is able to identify through the information it collects the identity of both TikTok and non-TikTok users alike.
>
> Counsel: Yes, they are able to identify it.
>
> The Court: Across the board, every single non-TikTok user, they can . . . track and identify who [the person is]?
>
> Counsel: Yes.

Dkt. No. 230 at 9:17–10:1. Defendants disputed the truth of this representation. *Id*. at 27:10–16.

Because of the potential significance of this representation and the dispute over its accuracy, the Court ordered Plaintiffs to file a supplement identifying the evidence in the record supporting their contention. Dkt. No. 232. A review of the evidence identified by Plaintiffs, Dkt. No. 235-1, confirms that they have overstated their argument.

Most of the record evidence on which Plaintiffs rely addresses the fact that the combination of a user's IP address and user agent (e.g., browser) can be used as identifiers. But identifier in this context means something narrower than what counsel represented. As Plaintiffs' expert Dr. Zubair Shafiq explained, "[t]he combination of IP address and user agent typically contains sufficiently distinguishing information . . . to be used as a unique identifier" that advertisers can use to identify the same user across different websites. Dkt. No. 179-2 at 9 ¶ 28.a & n.26. In other words, having multiple data points showing visits to different websites by the same combination of IP address and user agent tends to show that the same person visited both sites. *Id*. at 27 ¶ 62. Cookies can perform a similar function. *Id*. But, without more, this "identifying" information does not disclose *who* the person is. When the data belongs to a TikTok user whose personal information Defendants possess, Defendants can match the data collected by the Pixel to the user profile in their database and learn information about that user's browsing habits. Plaintiffs argued at the hearing, and Defendants do not appear to dispute, that "TikTok's own documents show that they need only the IP address and the user agent to match up a data point collected *to one of their users*." Dkt. No. 230 at 8:3–5 (emphasis added). On the other hand, when the data does not match Defendants' records of TikTok users because it belongs to class members (who, by definition, do not use TikTok), Plaintiffs produce no evidence that Defendants can identify who the person is that generated the data absent the collection of personally identifying information (PII) such as name, address, phone number, or email address linked to the IP address and user agent.

Plaintiffs cite to Dr. Shafiq's statement in his rebuttal report that "100.0% of the unmatched rows in [the sample of data collected by the Pixel that he analyzed] contained a hashed email address, hashed phone number, or one of the three types of cookies." Dkt. No. 198-2 at 33 ¶ 79. This assertion reiterates Dr. Shafiq's statement in his original report that "100.0% of the unmatched sampled data produced by TikTok for non-TikTok users in the United States contains at least one of [the user's email address, phone number, or TikTok cookies]. Dkt. No. 179-2 at 58–59 ¶ 82. But this assertion requires scrutiny. Paragraph 82 of Dr. Shafiq's report is supported by two footnotes identifying the data to support his assertion. *Id*. at 59 nn. 223 & 224. The more relevant of these, footnote 224, examines the same subset of Defendants' data sample that Dr. Shafiq elsewhere defines as "unmatched" data. *See id.* at 52 n.198 (identifying as "Criteria to identify unmatched data" the same criteria applied in footnote 224). In that data set, 0.8 percent of entries contained an email address, 0.5 percent contained a phone number, and 100 percent contained cookies. *Id*. at 59 n.224. Thus, saying that 100 percent of unmatched data contains phone numbers, email addresses, or

cookies is misleading as to the prevalence of PII given that at most 1.3 percent of the data contains phone numbers or email addresses.[4]

On this record, Plaintiffs have not supported their assertion that, from the data TikTok collects, Defendants can determine the actual identity of every non-TikTok user who visits a website with the Pixel installed. Merely learning that the same person visited other sites is not the same as discovering a user's identity.

III.

A class action is the exception to the rule requiring a lawsuit to be individually prosecuted. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 348 (2011). The moving party bears the burden of showing Rule 23 is satisfied. *See Marlo v. UPS*, 639 F.3d 942, 947 (9th Cir. 2011). Because of the onerous burdens class actions impose on defendants and the possibility that certifying a class will pressure defendants into settling nonmeritorious claims, "[c]lass certification is . . . not to be granted lightly." *Black Lives Matter Los Angeles v. City of Los Angeles*, No. 22-56161, 2024 WL 4048895, at *5 (9th Cir. Sept. 5, 2024) (published).

To justify a departure from the rule, the moving party must satisfy a two-part test. First, the plaintiffs must demonstrate through facts rather than allegations that the proposed class satisfies the requirements of Rule 23(a): (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy of representation by the class representatives and class counsel. Fed. R. Civ. P. 23(a); *see Doninger v. Pac. Nw. Bell, Inc.*, 564 F.2d 1304, 1309 (9th Cir. 1977) (mere allegations insufficient). "[C]ertification is proper only 'if the trial court is satisfied, after a rigorous analysis, that the prerequisites of Rule 23(a) have been satisfied,'" and the court's "rigorous analysis" may "entail some overlap with the merits of the plaintiff's underlying claim." *Dukes*, 564 U.S. at 350–51 (citation omitted). However, the Supreme Court has also cautioned that "Rule 23 grants courts no license to engage in free-ranging merits inquiries at the certification stage. Merits questions may be

[4] In footnote 223, Dr. Shafiq found that in a different subset of the data produced by Defendants, 10.4 percent of entries contained email addresses and 2.3 percent contained phone numbers. Dkt. No. 179-2 at 59 n.223. Plaintiffs have not adequately explained the significance of this data set or its relationship to the "unmatched" data in footnote 224. Regardless, even in the data set described in footnote 223, fewer than 13 percent of the entries include phone numbers or email addresses—far less than 100 percent.

considered to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied." *Amgen Inc. v. Connecticut Ret. Plans & Tr. Funds*, 568 U.S. 455, 466 (2013).

In addition to Rule 23(a), the plaintiffs must meet at least one of the three requirements of Rule 23(b). Here, Plaintiffs invoke Rule 23(b)(2) and (3). Rule 23(b)(2) permits certification when the defendant "has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief . . . is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). Rule 23(b)(3) permits a class to be maintained if "questions of law or fact common to class members predominate over any questions affecting only individual members" and if "a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3).

IV.

A.

Plaintiffs first seek certification of five related nationwide classes. Dkt. No. 177 (notice of motion); *see also* Dkt. No. 179-1 at 2–3 (describing classes).[5] Class 1 includes "[a]ll natural persons residing in the United States who visited a website using the TikTok Pixel from March 2022 to the present, and who have never been registered users of the TikTok app or held any TikTok account." Dkt. No. 177 at 1. Class 2 covers the subset of Class 1 that visited "a website using the TikTok Pixel and whose server uses the TikTok Events API" during the class period. *Id*. Class 3 encompasses the class members in Class 1 who also "had web browser or system settings turned on to block third-party cookies." *Id*. Class 4 covers the subset of Class 2 (i.e., users who visited sites that used both the Pixel and Events API) who also blocked cookies. *Id*. at 2. Class 5 covers the subset of Class 1 who visited a website that had the TikTok Pixel installed without "Search" configured as an optional event. *Id*. Plaintiffs also seek to certify a California subclass for each of these classes.

In the alternative, Plaintiffs move to certify a second set of classes, each tied to a particular website. Class 6 covers "[a]ll natural persons residing in the United States who visited the Rite Aid website from March 2022 to the present, and who

[5] The Court cites to the unredacted copies of the briefing filed under seal. Dkt. Nos. 179-1, 187-2, 198-1.

have never been registered users of the TikTok app or held any TikTok account." *Id*. at 3. Classes 7 through 10 are identical except that they cover the websites for Hulu, Etsy, Upwork, and Sweetwater, respectively. *Id*. at 3–4. For all but the Sweetwater class, Plaintiffs request certification of a California subclass. Plaintiffs also move to appoint Griffith, Shih, and Watters as class representatives for each of the classes to which they belong and to appoint their attorneys as class counsel.

B.

The parties have expended enormous resources on this motion: the eight expert reports alone span hundreds of pages. Yet Plaintiffs' submission leaves basic questions unanswered. After requesting certification of two different groups of classes in the alternative, Plaintiffs never address the alternative approaches, state a preference between them (although it is evident that they prefer the broader classes in Classes 1–5), or explain how they would be analyzed differently. Nor do Plaintiffs provide any argument specific to any of the 19 classes and subclasses they seek to certify. Instead, Plaintiffs address all their arguments to certification of a class in the abstract. Both parties' arguments appear to be aimed at the broadest proposed class—Class 1—which covers all non-TikTok users who have visited a website that uses the TikTok Pixel during the class period. Because hundreds of thousands of websites use this tool, it appears to be undisputed that Class 1 effectively covers all users of the internet in the United States who are not TikTok users.

To be certified, each class and subclass "must independently meet the requirements of Rule 23 for the maintenance of a class action." *Betts v. Reliable Collection Agency, Ltd.*, 659 F.2d 1000, 1005 (9th Cir. 1981). Thus, although Plaintiffs have not addressed them separately, the Court will evaluate each of Plaintiffs' alternative approaches.

1.

a.

Turning first to Classes 1–5, Plaintiffs have not shown that certification of these internet-wide classes is appropriate. The crux of Plaintiffs' claims is that Defendants violated their privacy and property rights by collecting valuable and sensitive personal information when they visited websites with the Pixel installed. Thus, the viability of Plaintiffs' claims depends on the nature of the information sent to Defendants. This information varies widely by website and by class

member, based at least on differences in (1) how each website chose to implement Defendants' software, (2) the nature of the website, and (3) the class member's activity on the site.

First, Plaintiffs produce evidence that the URL information sent to Defendants "can" contain PII, such as names, dates of birth, gender, phone number, email address, and physical address, as well as sensitive content including search queries. Dkt. No. 185-2 at 28 (decl. of Dr. Shafiq). But Plaintiffs do not contend that such information is captured by all—or even most—of the websites that use the Pixel.

Second, it appears self-evident (and Plaintiffs have not shown otherwise) that privacy concerns are not identical across all websites that use the Pixel. For example, it is not clear that a person visiting the Build-a-Bear website has the same expectation of privacy or is likely to disclose equally sensitive information as a visitor to the website for Rite Aid's pharmacy.[6] As Plaintiffs concede in their reply (although they dispute the implications), "Doordash.com is not Flirtfordate.com"—i.e., people have different expectations of privacy when ordering lunch than when seeking romantic partners. Dkt. No. 198-1 at 4. A visitor's reasonable expectation of privacy may also vary depending on the website's disclosures about how and with whom it shares information.

Third, it is not clear on this record that all visitors to the same website have identically strong claims. For example, Plaintiffs have not shown that a person who purchases office supplies on Rite Aid's website has the same privacy interests as a person who purchases birth control pills on the same site—or that a person who visits the website's homepage once has the same property interest in his or her data as someone who browses the site weekly, allowing Rite Aid (and Defendants) to track purchasing habits.

b.

This variation among class members and websites matters because the nature of the information Defendants receive about a class member is central to that individual's claims.

---

[6] That may explain why, even though the SAC alleges that Griffith visited both websites and includes class allegations as to both, Plaintiffs now seek certification of a website-specific class for Rite Aid but not for Build-a-Bear.

i.

As Plaintiffs acknowledge, their claims for invasion of privacy under the California Constitution and for intrusion upon seclusion require them to show that there was a reasonable expectation of privacy and that Defendants' intrusion was highly offensive. *In re Facebook, Inc. Internet Tracking Litig.* (*Facebook Tracking*), 956 F.3d 589, 601 (9th Cir. 2020). Plaintiffs emphasize that these elements are analyzed under an objective standard, *Rodriguez v. Google LLC*, No. 20-CV-04688, 2024 WL 38302, at *4 (N.D. Cal. Jan. 3, 2024) (citing *Shulman v. Grp. W. Prods., Inc.*, 18 Cal.4th 200, 232 (1998)), but objectivity does not dictate uniformity across the class. Consider two different hypothetical class members. The first regularly visits a pharmacy's website to search for and purchase medications related to sexual health, and the website provides her full browsing and shopping history to Defendants, along with her name, email address, and phone number. The second visits a toy store's website to browse teddy bears on one occasion, and the website sends Defendants the search terms and information about the class member's browser and IP address but no PII. Plaintiffs have not shown that these two members, objectively, have equal expectations of privacy in the information collected or that the collection was equally offensive in both cases.

In *Rodriguez*, on which Plaintiffs rely, the court found that differences among class members did not defeat predominance because all class members were Google users who selected certain privacy settings and alleged that Google collected data in violation of its representations about those settings, such that "the relevant inquiries are primarily Google's uniform disclosures and users' uniform conduct." *Id*. at *1, 5–6. Here, in contrast, class members did not encounter any disclosures from Defendants; they visited hundreds of thousands of different websites with varying disclosures about data collection; and they did not all take the same steps to safeguard their privacy.[7]

[7] At the hearing, Plaintiffs' counsel suggested that certifying only Class 3 would avoid these concerns because all class members would be people who selected an option to block cookies. While this approach might avoid the Court's concern about variation among class members' actions to safeguard their privacy, it is not obvious that it would address the other concerns expressed in the text accompanying the footnote. More fundamentally, Plaintiffs did not raise this argument in their motion, and Defendants have not had a fair opportunity to respond to it. The Court declines to consider this untimely argument.

*Facebook Tracking*, on which Plaintiffs also rely, is similarly unavailing. That decision, which did not address class certification, found that the plaintiffs had alleged viable privacy claims where Facebook tracked the activities of its users while they were logged out of the Facebook application, contrary to what its privacy disclosures suggested. The Ninth Circuit found that the plaintiffs had plausibly alleged a reasonable expectation of privacy in light of Facebook's misleading representations and the fact that Facebook knew the identity of its users and collected an enormous amount of individualized data on them. *Facebook Tracking*, 956 F.3d at 602–06. In that context, the court rejected Facebook's argument that the plaintiffs needed to identify specific sensitive information collected by Facebook, explaining that "*both* the nature of collection and the sensitivity of the collected information are important." *Id*. at 603. The court concluded that "there remain material questions of fact as to whether a reasonable individual would find the information collected from the seven million websites that employ Facebook plug-ins 'sensitive and confidential'" but that viewing the allegations in the light most favorable to the plaintiffs, it could not conclude that they had no reasonable expectation of privacy. *Id*. at 603–04. It is not obvious that the Ninth Circuit would have found class certification appropriate in *Facebook Tracking*, which settled before a class certification motion was filed. But even if it had, the facts of that case differ materially from those here. Among other things, the reasonable expectation of privacy alleged by Plaintiffs is not based on uniform representations to class members by Defendants, and the information collected from non-TikTok users cannot uniformly be linked to their identities because TikTok does not have user profiles for them.

---

Similarly, Plaintiffs' counsel advanced another new approach at the hearing: using a taxonomy of sensitive content (e.g., sexual content, illicit drugs, and sensitive social issues) to classify all websites that use the Pixel or Events API and certify a subset of the class that visited websites with sensitive content. This approach is found nowhere in Plaintiffs' briefs, and, in any event, does not appear to solve the problem. If RiteAid's website is classified as sensitive in the taxonomy because it includes sex-related products, then a class member who searches for pencils on RiteAid's website would be deemed to have engaged in a sensitive search, while a similarly situated class member who performs the same search on an office supply store's website would not. Regardless of the workability of this proposed approach, it is untimely, and the Court declines to consider arguments for a new proposed class to which Defendants have not had a fair opportunity to respond.

In sum, it appears that the existence of reasonable expectations of privacy and the requisite offensiveness will depend on the nature of the information collected from each class member. *See In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) ("Courts . . . have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms.").

ii.

Similarly, whether class members have a cognizable property interest in the information sent to Defendants for purposes of their statutory larceny and conversion claims turns on the nature of that information and whether it carries financial value. *See Facebook Tracking*, 956 F.3d at 600–01 (reversing dismissal of statutory larceny claim where plaintiffs alleged that their browsing histories carried financial value and that the defendant had profited by selling it to advertisers to generate revenue). Unlike the plug-ins at issue in *Facebook Tracking*, which were alleged to be used on seven million websites, *id*. at 603, Plaintiffs contend that the TikTok Pixel is installed on a few hundred thousand websites—still a large number, but a relatively small percentage of websites. *See* Dkt. No. 198-2 at 35 ¶ 83 (stating that the Pixel is present on 12 percent of websites). Plaintiffs have not shown that a market exists for only a small percentage of an internet user's browsing activity. Moreover, Plaintiffs have not shown that the volume and nature of information collected is uniform, or even similar, across the class. To the contrary, given that the class effectively encompasses all internet users in the nation who are not TikTok accountholders, it appears self-evident that there is wide variation in class members' browsing activity. While Plaintiffs have produced expert testimony tending to support their contention that a market exists for the comprehensive browsing history of an active internet user, they have not shown that a class member who briefly visits a few websites using the Pixel and shares no sensitive information has a marketable property interest in the data collected by the websites.

iii.

Whether class members have viable ECPA or CIPA claims likewise turns at least in part on whether the nature of the data shared qualifies it as "contents of [a] communication" covered by the statutes. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) (explaining that record information such as webpage addresses was excluded from the ECPA's definition of "contents" and insufficient to state a claim, even when it included PII); *Hammerling v. Google LLC*, 615 F.

Supp. 3d 1069, 1093 (N.D. Cal. 2022) ("URLs are record information [for purposes of CIPA] when they only reveal a general webpage address and basic identification information, but when they reproduce a person's personal search engine queries, they are contents.").

Plaintiffs' argument that whether URLs constitute "contents" is appropriate for classwide resolution is unpersuasive; they rely in their briefing on two decisions that did not involve class certification motions and that are distinguishable. *Gershzon v. Meta Platforms, Inc.* addressed the information obtained by the Meta Pixel on a particular website and found that the plaintiff had stated a plausible CIPA claim by identifying the specific information gathered on that site. No. 23-CV-00083, 2023 WL 5420234, at *13 (N.D. Cal. Aug. 22, 2023). *In re Meta Pixel Healthcare Litigation* found, in the course of denying a motion for preliminary injunction, that particular URLs transmitted from a group of hospital websites were contents within the meaning of the ECPA and CIPA. 647 F. Supp. 3d 778, 795, 798 (N.D. Cal. 2022). These decisions reinforce the conclusion that determining whether a URL constitutes "contents" turns on the specific information Defendants obtain from each website that uses the Pixel.

At the hearing, Plaintiffs also invoked *Campbell v. Facebook Inc.*'s discussion of ECPA and CIPA claims, in which the court stated that "the 'contents' issue provides no barrier to the predominance requirement" and that it was unnecessary to examine every URL. 315 F.R.D. 250, 265 (N.D. Cal. 2016). That case, however, is distinguishable; it addressed Facebook's practice of scanning the contents of users' private messages and recording any internet links in those messages. *Id*. at 255–56 ("Plaintiffs allege . . . that Facebook scans the content of their private messages, and if there is a link to a web page contained in that message, Facebook treats it as a 'like' of the page, and increases the page's 'like' counter by one. Plaintiffs further allege that Facebook uses this data regarding 'likes' to compile user profiles, which it then uses to deliver targeted advertising to its users. Plaintiffs allege that the messaging function is designed to allow users to communicate privately with other users, and that Facebook's practice of scanning the content of these messages violates the [ECPA and CIPA]."). The court distinguished *Zynga*, where the defendant collected URLs that functioned as addresses and therefore did not meet the definition of "contents," contrasting that with the facts in *Campbell* where the website URL was part of a message sent from one user to another. *Id*. at 265 ("In the messages at issue in this case, the sender is affirmatively choosing to share a certain webpage with the recipient, and the webpage itself is the 'substance, purport, or meaning' of the message. The fact that the substance of the message happens to be in the form of a URL does not

transform it from 'content' to 'record information.'"). Here, like in *Zynga* and unlike in *Campbell*, the URLs at issue are not part of messages sent by class members to third parties but rather reflect the addresses of the websites visited by the class members.

Plaintiffs also rely on *Brown v. Google LLC*, in which the court denied summary judgment on the named plaintiffs' ECPA claim while invoking a single example of a URL that contained content information. 685 F. Supp. 3d 909, 935 (N.D. Cal. 2023). That decision did not address class certification, however, and the court later denied the plaintiffs' motion to certify a damages class without addressing the question whether all class members had viable claims. *Brown v. Google, LLC*, No. 20-CV-3664-YGR, 2022 WL 17961497 (N.D. Cal. Dec. 12, 2022). *Brown* therefore does not support the argument that all class members can prevail on their ECPA and CIPA claims because Defendants collect "contents" from some of them.

In sum, whether a class member has had the contents of his or her communications collected by Defendants within the meaning of the ECPA and CIPA depends on the nature of the information collected.

c.

The variation in information gathered by different websites and as to different class members is fatal to certification of Classes 1–5 because it undermines typicality (at least on the limited record before the Court). As to the damages classes Plaintiffs seek to certify under Rule 23(b)(3), it also defeats commonality.

First, the named plaintiffs cannot show that their claims are typical of the class, precluding them from satisfying Rule 23(a)(3). Typicality does not require that the named plaintiffs' claims be identical to those of absent class members, but it does require that they be "reasonably co-extensive." *Castillo v. Bank of Am., NA*, 980 F.3d 723, 729 (9th Cir. 2020). "Measures of typicality include whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct." *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1116 (9th Cir. 2017) (cleaned up).

Plaintiffs have not met even this relatively low burden. They devote only one paragraph of their motion to typicality, conclusorily arguing that the named

plaintiffs are typical of the class because they visited websites using the Pixel and Events API, never had a TikTok account, and had their web browsers or systems set to block party cookies. Dkt. No. 179-1 at 5. That argument merely tracks the class definitions and shows that the named plaintiffs are members of the proposed classes. Plaintiffs provide no information about the nature or extent of their browsing activity on the identified websites or what information Defendants collected from Plaintiffs. Plaintiffs do not argue, much less provide evidence, that Defendants ever obtained any particularly sensitive information about them, or any of their PII (such as name, phone number, or email address), through Plaintiffs' online activity on websites that used the Pixel or Events API.

Indeed, Plaintiffs generally gloss over the differences among class members' internet activity. They rely on Dr. Shafiq's declaration stating that the average internet user visits about 50 webpages each day and that the TikTok Pixel is present on 12 percent of its websites, from which he calculated that there is a 100 percent chance that a class member visited a website on which the Pixel collects search terms during a year and a 12.4 percent chance that a class member does so in a day. Dkt. No. 198-2 at 35 ¶ 83. But Plaintiffs have not shown that the average internet user's online activity represents the activity of all class members. Dr. Shafiq's approach relies on several assumptions that Plaintiffs have not shown to be true. For example, it is not self-evident that the average internet user engages in the same activity as the average internet user who does not use TikTok. Nor have Plaintiffs shown that the 12 percent of websites that employ the Pixel represent 12 percent of internet traffic (much less 12 percent of the websites visited by class members) or that internet users who visit 50 webpages a day are visiting 50 new sites each day. Even apart from all these assumptions, it appears indisputable that some individuals use the internet more than average and others less.[8] Reliance on averages does little to inform whether all class members are similarly situated (or, relatedly, whether the named plaintiffs are typical of the class).

In the absence of any information about the variation in internet activity among class members or about how the named plaintiffs' activity and the data

[8] Dr. Shafiq also performed calculations based on "conservative" assumptions about a class member who visits only five websites each day. Dkt. No. 198-2 at 35 ¶ 84. But Plaintiffs have not produced any evidence suggesting that every class member (i.e., every person in America who has visited a website with the Pixel installed and who does not use TikTok) visits at least five websites each day or even uses the internet daily.

collected from them compares to others in the class, Plaintiffs' mere showing that they fit within the class definitions is inadequate to establish that their claims are typical of the class. Indeed, because the named Plaintiffs have not produced evidence of any data collected from them, it is not even clear that they have suffered any cognizable injury, while it appears that at least some class members may have. *See Dukes*, 564 U.S. at 348–49 (to justify departure from the usual rule that litigation is conducted on behalf of named plaintiffs only, "a class representative must . . . possess the same interest and suffer the same injury as the class members") (cleaned up). Plaintiffs' conclusory one-paragraph argument on typicality is insufficient to meet their burden to show that they have suffered the same injury as other class members.[9] Thus, Plaintiffs' motion must be denied for failure to satisfy Rule 23(a), which precludes certification of classes for either injunctive relief or damages.

Second, even if Plaintiffs could satisfy Rule 23(a), the same problems identified above also preclude certification of a damages class under Rule 23(b)(3) because Plaintiffs cannot show that common questions predominate over individual issues. Because the viability of class members' claims depends in large part on the nature of the information sent to Defendants, the Court would have to consider what information is shared by each website on which Plaintiffs attempt to predicate liability, and possibly even the information collected as to each class member. With hundreds of thousands of websites that use the Pixel and a class that essentially encompasses all internet users in the United States who do not have TikTok accounts, this task would overshadow any benefits to be gained from addressing common questions through class certification.

d.

Plaintiffs attempt to overcome these conclusions in two ways. First, they try to obscure the differences in the data collected across different websites to argue that the same information is uniformly sent to Defendants. Plaintiffs rely on expert testimony that classifies the information into seven categories of data that are

[9] The Court does not reach Defendants' additional arguments against typicality, including those addressing Plaintiffs' subjective privacy expectations, the varied disclosures provided by different websites, Plaintiffs' continued use of websites after learning that the Pixel sent their browsing information to Defendants, and whether the named plaintiffs can represent class members who visited websites not visited by the named plaintiffs.

automatically sent to Defendants nearly every time someone visits a website with the Pixel installed: (1) timestamp, (2) IP address, (3) user agent, (4) cookies, (5) URL, (6) event information, and (7) content information. Dkt. No. 185-2 at 24–37, 47. But classifying the information with these high-level categories, without more, says little about what matters—the sensitivity and substance of the browsing information collected. Much of this information is not protected. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (explaining in Fourth Amendment case that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information"); *see also Facebook Tracking*, 956 F.3d at 604 n.7 ("[W]e have . . . found analogies to Fourth Amendment cases applicable when deciding issues of privacy related to technology."). Plaintiffs' expert emphasizes that a URL *can* contain sensitive information, but Plaintiffs have not shown that the URLs sent to Defendants based on their own browsing history *did*.[10] It is the contents of the URLs, not the mere fact that URLs were sent, that matters. As the Ninth Circuit has explained in the context of an ECPA claim:

> Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication. But the referer header information at issue here includes only basic identification and address information, not a search term or similar communication made by the user, and therefore does not constitute the contents of a communication.

[10] From his review of sample data, Plaintiffs' expert concluded that the probability that TikTok Pixel collects search terms from a page URL is less than 2.5 percent (from which he calculated that each class member would have had a search term collected at least once in a year). Dkt. No. 198-2 at 35 ¶ 83. He did not offer an opinion as to what percentage of those search terms were sensitive. As examples of sensitive data, Plaintiffs show that Defendants obtained URL data showing a search for "crotchless lingerie" on Etsy's website and that the Pixel can collect information about a search for "pregnancy test" on Rite Aid's website through the URL. Dkt. No. 179-1 at 10. Plaintiffs do not allege or provide evidence that any named plaintiff searched for similarly sensitive items on either website—or on any other site that uses the Pixel.

*Zynga*, 750 F.3d at 1108–09. Because Plaintiffs address the uniformity of websites' collection processes at such a high level that it obscures whether protected information has actually been shared, they have not met their burden to show that the named plaintiffs' claims are typical of the class or that common issues predominate.

The second prong of Plaintiffs' attack points to the numerous common issues present in this case. To be sure, there are common questions about how Defendants' technology works, how Defendants interact with the website owners who use the Pixel, what information they collect, and what they do with that information, among other things. But "[t]he predominance inquiry is 'more demanding' than the commonality inquiry." *DZ Rsrv. v. Meta Platforms, Inc.*, 96 F.4th 1223, 1233 (9th Cir. 2024) (citing *Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 624 (1997)). Plaintiffs must show not only that there are common questions (or even a large number of common questions), but also that those questions "predominate over any questions affecting only individual members." Fed. R. Civ. P. 23(b)(3). The focus of this inquiry "is whether a proposed class is sufficiently cohesive to warrant adjudication by representation." *Castillo*, 980 F.3d at 730 (cleaned up). In considering predominance, "the court must ensure that the class is not defined so broadly as to include a great number of members who for some reason could not have been harmed by the defendant's allegedly unlawful conduct." *Id*. (cleaned up).

As explained above, the proposed classes include virtually all internet users in the United States who are not TikTok users. Plaintiffs have not shown that Defendants have received sensitive information from all, or even most, class members. Indeed, on this record, it is possible that the vast majority of class members have suffered no cognizable harm. Because the viability of each class member's claims turns on the contents of the information collected from his or her browsing activity, which in turn depends on the implementation of the Pixel and Events API on each particular website that uses those tools, questions affecting individual class members would predominate over common questions.

e.

Plaintiffs' failure to establish typicality precludes certification of Classes 1–5 and the related subclasses. Their failure to establish predominance provides a further bar to certification of damages classes. Accordingly, the Court need not address the remaining requirements of Rule 23.

2.

The website-specific classes Plaintiffs propose in the alternative (Classes 6–10) do not present all the same obstacles to certification as the internet-wide classes, and it is conceivable that Plaintiffs might be able to show certification is proper as to those classes.[11] But they have not met their burden to do so on this record. Indeed, other than a passing reference to the alternatively requested classes, Plaintiffs' briefing ignores them entirely—as did their argument at the hearing. Plaintiffs have not made any attempt to show that their browsing activity on the Rite Aid, Hulu, Etsy, Upwork, or Sweetwater websites was typical of visitors to those sites, nor that the information collected from them was typical. And Plaintiffs' damages models are predicated on the claimed value of class members' browsing history on the internet as a whole; their damages expert made no attempt to quantify the value either to Plaintiffs (for purposes of restitution) or to Defendants (for purposes of disgorgement) of the information Defendants received from the Pixel on any of the specified websites in isolation. Dkt. No. 179-3 (decl. of Russell Magnum); *see Comcast Corp. v. Behrend*, 569 U.S. 27, 34 (2013) (explaining that certification under Rule 23(b)(3) requires damages to be capable of measurement on a classwide basis).

Thus, Plaintiffs likewise have not satisfied the requirements of Rule 23(a) or (b)(3) in connection with Classes 6–10 and the associated California subclasses.

3.

In a single paragraph at the end of their motion, Plaintiffs include an alternative request for classwide determination of specific issues under Rule 23(c)(4), which provides that "[w]hen appropriate, an action may be brought or maintained as a class action with respect to particular issues." *See Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1234 (9th Cir. 1996) ("Even if the common questions do not predominate over the individual questions so that class certification of the entire action is warranted, Rule 23 authorizes the district court in appropriate cases to isolate the common issues under Rule 23(c)(4)(A) and

[11] The Court does not intend to suggest that a renewed motion for certification of website-based classes *would* be granted if Plaintiffs can show typicality; Defendants have raised additional arguments against certification that the Court does not reach at this time.

proceed with class treatment of these particular issues."). Plaintiffs argue that there are "numerous" issues appropriate for classwide determination, but they identify only three:

- [Whether t]he Pixel and Events API each operates to collect data of class members that visit websites unaffiliated with TikTok, including certain baseline data automatically collected regardless of the websites' own configurations;
- Whether and by how much Defendants were unjustly enriched from the Pixel's and/or Events API's unauthorized data collection;
- Whether class and subclass members suffered lost value of their PII as a result of the Pixel's and/or Events API's unauthorized data collection.

Dkt. No. 179-1 at 22.

The first issue appears to be a red herring; there is no dispute that the Pixel and Events API collect data of class members who visit websites that have the tools installed. For the second issue, the question of unjust enrichment (which the Court has found does not constitute an independent cause of action) from "unauthorized" data collection is predicated on liability findings that Plaintiffs have not shown can be established classwide. Class treatment of remedies is therefore premature. The sole case cited by Plaintiffs denied class certification and merely noted the possibility that liability might be able to be resolved classwide, to be followed by adjudication of damages. *In re Apple iPhone Antitrust Litig.*, No. 11-CV-6714, 2022 WL 1284104, at *17 (N.D. Cal. Mar. 29, 2022). As for the third issue, Plaintiffs have not shown that the lost value of class members' PII can be determined classwide—they have not even identified a named plaintiff whose PII was obtained by Defendants.

Accordingly, Plaintiffs have not identified any issues suitable for classwide resolution at this stage. And even if they were to identify isolated issues that *could* be resolved classwide, they have not shown that the Court *should* find that this is an appropriate case in which to exercise its discretion to adjudicate those issues classwide.

V.

Because Plaintiffs have not met their burden under Rule 23 to show that any of the proposed classes should be certified, their motion is denied.

Date: September 9, 2024

Stanley Blumenfeld, Jr.
United States District Judge